Commonwealth of Massachusetts
Center for Health Information & Analysis (CHIA)
Data Management Plan for Non-Governmental Data Use

This Data Management Plan is to be completed by non-governmental applicants for APCD and Case Mix Data, except for applicants seeking de-identified data, as that term is defined in 957 CMR 5. This form should be completed by the applicant's Chief Information Security Officer, Chief Privacy Officer, legal counsel, or an officer with sufficient knowledge of the Applicant's data privacy and security practices and authority to bind the organization.

GENERAL INFORMATION

APPLICANT INFORMATION	
Applicant (principal investigator/project lead)	
Title:	
Organization:	
Project Title:	
Mailing Address:	
Telephone Number:	
Email Address:	
CISO/CPO/Counsel/Officer responsible for Data Privacy and/or Security	
Email Address of Officer responsible for Data Privacy and/or Security	
Data Request Submission Date:	
Data Management Plan Submission Date (if different from Data Request date):	
DMP Revision Dates:	

Data Management Plan

A full Data Management Plan should be completed by any collaborating organization that will receive a copy of the CHIA files sought in the Data Request.

If your organization has an approved Data Management Plan on file with CHIA, you may submit that form and annotate it to reflect any proposed changes to the approved practices. Applicants should also note if they are providing to CHIA a Data Management Plan previously approved by CMS.

1. **PHYSICAL POSSESSION AND STORAGE OF CHIA DATA FILES**

1.1. Who will have the main responsibility for organizing, storing, and archiving the data? Please provide name(s) and job title(s).

1.2. Describe how your organization maintains a current inventory of CHIA data files, if any.

1.3. Describe how your organization binds all members (i.e., organizations, individual staff) of research or project teams to specific privacy and security rules in using CHIA data files. This includes, for example, confidentiality agreements and non-disclosure agreements.

1.4. Provide details about how, and by whom, your organization will notify CHIA of any project staffing changes.

1.5. Describe your organization's training programs that are used to educate staff on how to protect CHIA data files.

1.6. Explain the infrastructure (facilities, hardware, software, other) that will secure the CHIA data files.

1.7. Describe the policies and procedures regarding the physical possession and storage of CHIA data files.

1.8. Explain your organization's system or process to track the status and roles of the research team.

1.9. Describe your organization's physical and technical safeguards used to protect CHIA data files (including physical access and logical access to the files).

2. DATA SHARING, ELECTRONIC TRANSMISSION, DISTRIBUTION

2.1. Describe your organization's policies and procedures regarding the sharing, transmission, and distribution of CHIA data files.

2.2. If your organization employs a data tracking system, please describe.

2.3. Describe the policies and procedures your organization has developed for the physical removal, transport and transmission of CHIA data files.

2.4. Explain how your organization will tailor and restrict data access privileges based on an individual's role on the research team.

2.5. Explain the use of technical safeguards for data access (which may include password protocols, log-on/log-off protocols, session time out protocols, and encryption for data in motion and data at rest).

2.6. Are additional organizations involved in analyzing the data files provided by CHIA?

If so, please review the Collaborator Checklist (see below) for guidance and considerations to include in the Data Management Plan, and indicate below how these organizations' analysts will access the data files:

__ VPN connection
__ Will travel to physical location of data files at requesting organization
__ Request that a copy of the data files be housed at second location
__ Other:

2.7. If an additional copy of the data will be housed in a separate location, please describe how the data will be transferred to this location. (Also, please ensure you have included information on how the data will be managed at this location under the appropriate subsections of the Data Management Plan.)

3. **DATA REPORTING AND PUBLICATION**

3.1. Who will have the main responsibility for notifying CHIA of any suspected incidents wherein the security and privacy of the CHIA data may have been compromised? Please describe and identify your organization's policies and procedures for responding to potential breaches in the security and privacy of the CHIA data.

3.2. Explain how your organization's data management plans are reviewed and approved by your organization.

3.3. Explain whether and how your organization's data management plans are subjected to periodic updates during the DUA period.

3.4. Please attest to the CHIA cell suppression policy of not publishing or presenting tables with cell sizes less than 11 to anyone who is not an authorized user of the data.

__ I agree. (Please place your initials on the line.)

4. COMPLETION OF RESEARCH TASKS AND DATA DESTRUCTION

4.1. Describe your organization's process to complete the Certificate of Destruction form and policies and procedures to dispose of data files upon completion of its research.

4.2. Describe your organization's policies and procedures used to protect CHIA data files when individual staff members of project teams (as well as collaborating organizations) terminate their participation in projects (which may include staff exit interviews and immediate access termination).

4.3. Describe policies and procedures your organization uses to inform CHIA of project staffing changes, including when individual staff members' participation in research projects is terminated, voluntarily or involuntarily.

4.4. Describe your organization's policies and procedures to ensure that CHIA data and any derivatives or parts thereof are not used following the completion of the project.

COLLABORATOR CHECKLIST

Please note –this checklist is for guidance purposes only and for organizations that are involving an additional organization as part of their project. The checklist identifies data safeguard practices and considerations of the collaborating organization that should be indicated in the data requestor's Data Management Plan. All questions may not apply but are dependent upon the data sharing arrangement between the organizations involved in the research project.

Information should be indicated for <u>each</u> collaborating organization that will have access to CHIA data files.

A. Access to Identifiable and De-identifiable Files

1. What is the name of the collaborating organization?

2. How will the collaborating organization access the CHIA data (secure VPN, a physical copy on site at the collaborating organization, traveling to the DUA holder's site, etc.)?

3. Who are the project staff from the collaborating organization? Indicate if each project staff member will have access to raw data, analytic files, or output with cell sizes less than 11. (*Please ensure that these individuals and data access rights are listed in the Project Staff list.*)

4. What binding agreements are required of the project staff members from the collaborating organization?

5. What training is required of project staff members from the collaborating organization?

6. How will the collaborating organization notify the DUA holder of changes in staff who are participating on the project team?

7. Will the researchers from the collaborating organization abide by the DUA holder's project rules or the policies of their employing organization?

B. Access to Protected Health Information

1. Will the collaborating organization have access to PHI?

If yes, please provide the following required details:

a. Will the collaborating organization have the ability to download and store a copy of the CHIA data?

b. Does the collaborating organization intend to backup the data? If so, has the collaborating organization developed a backup arrangement and are the back-up copies maintained at a second location?

c. Who is responsible for maintaining the security and distribution of the CHIA data at the collaborating organization?

d. Does the collaborating organization maintain an inventory of the CHIA data?

e. How will the collaborating organization tailor and restrict data access?

f. Please describe the collaborating organization's physical and technical safeguards used to protect CHIA data files (including physical access and logical access to the files).

g. Please describe the collaborating organization's infrastructure, operating systems, and hardware that will be used to secure the CHIA data.

h. How will the collaborating organization dispose of electronic copies of the data?

C. Physical Copies of CHIA Data

Please note - if the collaborating organization will maintain a separate copy of the CHIA data, the collaborating organization is required to complete a full Data Management Plan.

1. Will a separate copy of the CHIA data be housed at the collaborating organization's location?

2. How will the collaborating organization receive the CHIA data?

XIII. ASSURANCES

Applicants requesting and receiving data from CHIA pursuant to 957 CMR 5.00 ("Data Recipients") will be provided with data following the execution of a data use agreement that requires the Data Recipient to adhere to processes and procedures aimed at preventing unauthorized access, disclosure or use of data, including the processes and procedures outlined in this Data Management Plan.

Data Recipients are further subject to the requirements and restrictions contained in applicable state and federal laws protecting privacy and data security, and will be required, as a condition of receipt of CHIA data, to agree to establish and maintain appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use or access to it. The safeguards shall provide a level and scope of security that is consistent with 45 CFR § 164.530(c) and not less than the level and scope of security requirements established by the Office of Management and Budget (OMB) in OMB Circular No. A-130, Appendix III--Security of Federal Automated Information Systems **http://www.whitehouse.gov/omb/circulars/a130/a130.html)** as well as Federal Information Processing Standard 200 entitled "Minimum Security Requirements for Federal Information and Information Systems" **(http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf);** and, Special Publication 800-53 "Recommended Security Controls for Federal Information Systems" **(http://csrc.nist.gov/ publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf)**.

Data Recipients must notify CHIA, as soon as practicable, of any unauthorized use or disclosure of CHIA data.

The undersigned agrees that the Applicant and any collaborating oranizations will adhere to the Data Management Plan described herein and will notify CHIA of any material changes in Data Management pertaining to an approved project that involves the use of CHIA Data.

CISO/CPO/Counsel Signature:	
Title	
Printed Name:	
Authorized Agent Signature	
Authorized Agent Title	
Printed Name:	
Original DMP Submission Date:	
Dates DMP Revised:	